UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FEDERAL TRADE COMMISSION,	)	
	)	
Plaintiff,	)	Case No. 13-cv-1527
	)	
v.	)	Judge John W. Darrah
	)	
SUBSCRIBERBASE HOLDINGS, INC., a South Carolina corporation, *et al.*,	)	Magistrate Judge Geraldine Soat Brown
	)	
Defendants.	)	
	)	

DECLARATIONS AND EXHIBITS IN SUPPORT OF FEDERAL TRADE COMMISSION'S MOTION FOR TEMPORARY RESTRAINING ORDER WITH OTHER EQUITABLE RELIEF AND ORDER TO SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE

Declaration of Douglas M. McKenney PX1,
Investigator, Federal Trade Commission Atts. A-T

Certification of Authenticity of Business Records by Sergio Hernandez PX2,
Executive Vice President, NameCheap, Inc. attached records

Certification of Records of Regularly Conducted Activity by Vivian Cahill PX3,
DNC Holdings, Inc. attached records

Certification of Records of Regularly Conducted Activity by Saquonna Wheeler PX4,
Cox Communications, Inc. attached records

Certificate of Authenticity by Chi Nguyen PX5,
Custodian of Records, Google Inc. attached records

Declaration of Lisa Smith PX6
Vice President of Enterprise Customer Care, Best Buy Stores, L.P.

Declaration of Cheri Kerstetter PX7
Lead Billing Ops Manager, Global Fraud Management Organization, AT&T Services, Inc.

Declaration of Michael F. Altschul PX8
Senior Vice President and General Counsel, CTIA—The Wireless Association

Declaration of Donald B. Farren PX9
Certified Public Accountant contracted by CTIA—The Wireless Association

PX 1

DECLARATION OF DOUGLAS M. MCKENNEY
PURSUANT TO 28 U.S.C. § 1746

I, Douglas M. McKenney, hereby declare as follows:

1. My name is Douglas M. McKenney. I am a United States citizen over eighteen years of age. I am an investigator with the Federal Trade Commission ("FTC"). I have been employed by the FTC for approximately eight years. My business address is Federal Trade Commission, Midwest Region, 55 West Monroe Street, Suite 1825, Chicago, Illinois 60603.

2. As an investigator, my duties include monitoring and investigating persons and companies that are suspected of engaging in unfair or deceptive acts or practices in violation of the Federal Trade Commission Act and any other laws or rules that the FTC enforces. I also am custodian of documents and records that the FTC obtains during the course of investigations to which I am assigned. In the course of my employment, I participated in an investigation of a series of websites that promoted "free" merchandise. That investigation included the following entities and individuals: SubcscriberBASE Holdings, Inc. ("SubscriberBASE Holdings"); SubscriberBASE, Inc. ("SubscriberBASE"); Jeffrey French; All Square Marketing, LLC ("All Square Marketing"); Threadpoint, LLC ("Threadpoint"); PC Global Investments, LLC ("PC Global"); Slash 20, LLC ("Slash 20"); Brent Cranmer; Christopher McVeigh; and Michael Mazzella. In the course of this investigation, I acquired personal knowledge and information about the facts stated herein, and, if called upon as a witness, I would testify competently thereto.

AFFILIATE MARKETING

3. During this investigation and past FTC investigations, as well as from information culled from public sources, I have learned that Internet advertising often involves affiliate marketing and have become familiar with that practice.

4. In affiliate marketing, a seller of goods or services (typically called the "merchant") uses other firms or individuals (the "affiliates") to market the merchant's goods or services by attracting customers to the merchant's websites. The merchant rewards one or more affiliates for each visitor or customer generated by the affiliate's own marketing efforts. An affiliate is rewarded either directly by the merchant whose product the affiliate advertises or by a third party (the "affiliate network") that serves as an intermediary between the affiliate and the merchant. In some cases, multiple affiliate networks or other intermediaries separate the affiliate from the merchant. Affiliates can earn commissions in different ways, but most of those commissions are classified as either "cost per click" and "cost per action." An affiliate earns a "cost per click" commission by inducing a consumer to click on a link that leads the consumer to the merchant's website. An affiliate earns a "cost per action" commission when a consumer takes a specific action, such as purchasing a product, signing up for a free trial of the product, or submitting identifying information. That identifying information can include the consumer's email address or zip code, so that when the consumer submits the requested information on the website of the merchant or an affiliate network, the affiliate earns a flat commission. To determine the amount of reward for the affiliate, the merchant or the affiliate network tracks the number of consumers drawn to the merchant's site by the affiliate and/or the action(s) taken by those consumers that can be attributed to the affiliate.

5. In affiliate marketing, an affiliate generally tries to attract consumers to a merchant's website and generate product sales. The affiliate can attract consumers to the merchant's website in a number of different ways, including email marketing, display advertising, and commercial text messages. In some cases, clicking on a link in an email, display advertisement, or commercial text message takes a consumer directly to the merchant's website. In others, the links take consumers to a website set up by an affiliate, who uses that website to further attract visitors to the merchant's website, or to another intermediary website that in turn leads to the merchant's website. The affiliate's website and any other intermediary websites often will contain representations about the merchant's products or services.

BACKGROUND

6. As part of this investigation, pursuant to Section 20 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 57b-1, the FTC issued Civil Investigative Demands ("CIDs") to parties having information relevant to the investigation. I am the custodian of documents produced pursuant to the CIDs issued in this investigation, and I personally have reviewed these documents.

7. In the course of this investigation, FTC staff in the Midwest Regional Office used two different methods of capturing the contents of a website:

a. FTC staff used the software program Adobe Acrobat 9 Professional ("Adobe") to capture websites. One of Adobe's numerous software tools allows users to convert the contents of a web page into a PDF file. The conversion process includes any JPEG images, text files, image maps, as well as other associated files from the original web page; and

b. FTC staff also used TechSmith Corporation's software program Snagit to capture websites. Snagit is a screen capture program that allows users to select and capture the contents of any window or web page.

WEBSITE CAPTURES

wonbestbuy.com - myrewards2day.com - bestdigitalrewards.com

8. On or about August 24, 2012, from the FTC's office in Chicago, based on consumer complaints of text message spam, I entered wonbestbuy.com into a web browser, and was taken to that publicly available website. According to my web browser, this page was entitled "Free $1000 BestBuy Gift Card." I used Adobe to capture the website wonbestbuy.com, as well as other websites linked to from this website. True and correct printouts of this captured website and other websites linked to from this website dated August 24, 2012, are attached hereto as **McKenney Att. A**. Undercover information has been redacted from the attachment.

9. This website displayed a message at the top of the web page stating "Get a Free $1,000 Best Buy Gift Card." Beneath that message was an image of a Best Buy gift card, an image of a Canon camera, and an image of an Apple iPad. Beneath those images was an instruction to enter my "Code:" with a blank next to it. Based on the text message, I entered a code then pressed a button labeled "CONTINUE."

10. I was redirected to the publicly available website http://bestbuy.myrewards2day.com/p1.php?reqid=3080005&affid=14&oid=13&s1=2580&s2=102b970ba3aaee7125d68890a9c7b2&pre_q=&email=. This website displayed a message at the top of the web page stating "GET A FREE $1000 BEST BUY GIFT CARD." The website also stated, "Congratulations! You Qualify for a FREE $1,000 Best Buy Gift Card." Between these two messages were several images, including an image of a person that appeared to be a Best Buy employee as well as image of a Best Buy gift card, a flat-screen television, an Apple iPad,

another Apple product such as an iPhone or iPod, and a Canon camera. The website instructed, "Enter Your E-mail Address:" and included a space in which to do so. Beneath that space was a button marked "CONTINUE." McKenney Att. A, at 2.

11. At the bottom of the web page, in smaller type, was the following text:

> **This Gift Redemption Program is an independent rewards program for consumers and is not affiliated with, sponsored by or endorsed by any of the listed products or retailers. Trademarks, service marks, logos, and/or domain names (including, without limitation, the individual names of products and retailers) are the property of their respective owners.** THE FOLLOWING IS A SUMMARY OF PROGRAM REQUIREMENTS. SEE TERMS & CONDITIONS FOR COMPLETE DETAILS. Members are being accepted subject to the following Program Requirements: 1) Must be a legal US resident; 2) must be at least 18 years old or older; 3) must have a valid email and shipping address; 4) Eligible members can receive the incentive gift package by completing two reward offers from each of the Silver and Gold reward offer page options and nine reward offers from the Platinum reward offer page options and refer 3 friends to do the same. Various types of reward offers are available. Completion of reward offers most often requires a purchase or filing a credit application and being accepted for a financial product such as a credit card or consumer loan. The following link illustrates a Representative Sample of reward offers by group along with monetary and non-monetary obligations. Failure to submit accurate registration information will result in loss of eligibility. This promotion is administered solely by this website. The manufacturers and retailers of the gift items offered through our programs have not endorsed this promotion and are not affiliated with the promotion in anyway. Please read the Terms and Conditions for complete program details. Your information will be shared with our marketing partners. Please read the Privacy Policy for more details.

In this text, the underlined terms "Representative Sample," "Terms and Conditions," and "Privacy Policy" all were hyperlinks. Several of the additional web pages on myrewards2day.com had identical or nearly identical text with links to identical or nearly identical documents.

12. I clicked on the hyperlink "Representative Sample," and was redirected to the publicly available website http://mywebrewardsclub.com/offers.php. McKenney Att. A, at 3-7.

13. From the web page, described in paragraph 10 above, on the website http://bestbuy.myrewards2day.com/p1.php, I also clicked on the hyperlink "Terms and Conditions," and was directed to the publicly available website http://bestbuy.myrewards2day.com/common/terms.php. McKenney Att. A, at 8-10.

14. From the web page, described in paragraph 10 above, on the website http://bestbuy.myrewards2day.com/p1.php, I also clicked on the hyperlink "Privacy Policy," and was directed to the publicly available website http://bestbuy.myrewards2day.com/common/privacy.php. McKenney Att. A, at 11-13.

15. I entered an undercover email address, clicked on the button marked "CONTINUE," and was redirected to the website http://bestbuy.myrewards2day.com/common/rpa.php?stc=2&oid=13. This page stated, "Congratulations! Tell us where to send your $1000 BestBuy [sic] Gift Card!". The page requested additional personal information from me, including my gender, name, address, date of birth, and cell phone number. The page also asked me certain questions, such as "Are you diabetic?", with buttons labeled "yes" and "no" next to the question. Beneath the blanks for this information was a button marked "CONTINUE." McKenney Att. A, at 14-15.

16. I filled in the required fields using undercover information and I was then sent through several additional pages on the website http://bestbuy.myrewards2day.com. These additional pages included "optional offers". Each additional page was labeled according to the "Step" I had reached, such as "Step 3" or "Step 4." McKenney Att. A, at 16-18.

17. After skipping these optional offers, I was redirected to a page on the website http://bestdigitalrewards.com labeled "Last Step." This page stated, "Tell us where to ship your $1000 BestBuy [sic] Gift Card." Below this text, the page displayed a pre-filled FedEx shipping

label containing the undercover name and address I used on the previous website. To the left of this label was an image of a Best Buy gift card with the message "$1000 Best Buy Gift Card!" above it. To the right of the label was an image of a FedEx delivery truck with the message, "Includes Free Shipping." Beneath my undercover information was a button labeled "Send It!" McKenney Att. A, at 19.

18. I clicked the button labeled "Send It!" for the shipping of my $1,000 Best Buy Gift Card, and the web page immediately expanded. The undercover information I had entered continued to be displayed at the top of the page, but now I was told to complete any two third-party offers listed on that page. I also proceeded to the next two pages, where there were more offers to sign up for, and where I was informed that I needed to sign up for additional offers to claim the gift card. Most of the offers listed on these pages stated that I needed to pay a fee to participate. The later pages stated, "Free $1000 BestBuy Gift Card Reserved For:" above my undercover contact information. McKenney Att. A, at 20-31.

tbtt.biz - myrewardshouse.com - bestdigitalrewards.com

19. On or about July 21, 2012, FTC staff received, on a cell phone, an unsolicited text message from (316) 200-5559 stating, "Your entry in our drawing WON you a free $1,000 Best Buy GiftCard! Enter "614" at www.bestbuy.com.tbtt.biz so we can ship it to you immediately." FTC staff took a picture of the text message. I used Adobe and Snagit to capture this website listed in this text message as well as other websites linked to from that website. True and correct printouts of the text message and the websites I captured are attached hereto as **McKenney Att. B**. Undercover information has been redacted from the attachment.

20. On July 23, 2012, from the FTC's office in Chicago, I entered www.bestbuy.com.tbtt.biz, the website listed in the unsolicited text message, into a web browser and visited the publicly available website. McKenney Att. B, at 2.

21. This website stated at the top of the page "Get a $1,000 Bestbuy Gift Card!" Below that message, the page stated "118 of 1000 left" next to an image of a Best Buy gift card. Beneath that image was the instruction "Please enter your code below" and a blank in which to do so, with a button labeled "Continue" next to it. I entered the code "614" from the text message and pressed continue. This website then displayed the message "Your code is being validated… please stand by!" followed by, "You have a Winning Code! Now sending you to claim your giftcard!" McKenney Att. B, at 3-4.

22. I then was redirected to the website http://bestbuy.myrewardshouse.com/p1.php?reqid=1263572&affid=8&oid=13&s1=2548&s2=102357f8d2ae1ac64921048a27383a. The website stated "Get a FREE $1000 Best Buy Gift Card." Below and to the left of this message was another message stating, "Congratulations! You Qualify for a Free $1,000 Best Buy Gift Card." Positioned between these two messages were several images, including the Best Buy logo, a photograph of a supposed Best Buy employee, an image of a Best Buy gift card, and images of a Samsung flat-screen television, an Apple iPad, an Apple iPhone, and a Canon camera. Beneath the two messages, the website instructed, "Enter Your E-mail Address:" and included a space in which to do so. Beneath that space was a button marked "Continue." At the bottom of this web page and several additional pages attached as McKenney Att. B was identical or nearly identical text to the text quoted in paragraph 11, above, as well as links to identical or nearly identical "Representative Sample," "Terms and

Conditions," and "Privacy Policy" pages described in paragraphs 12 through 14 above. McKenney Att. B, at 5.

23. I inputted an undercover email address in the blank, then pressed "Continue." I immediately was directed to another page on the same website, http://bestbuy.myrewardshouse.com/common/rpa.php?stc=2&oid=13. That website stated, "Congratulations! Tell us where to send your $1000 BestBuy Gift Card!" Beneath that message, the website requested additional personal information from me, including my gender, name, address, email address, date of birth, cell phone number. I filled in the required fields using undercover information and I was then directed through an additional page on the website http://bestbuy.myrewardshouse.com, where I was asked to "Confirm" my cell phone number. McKenney Att. B, at 6-8.

24. I then was redirected to a webpage on the website http://bestdigitalrewards.com. This page told me that I was at the "Last Step," and instructed me to "Tell us where to ship your $1000 BestBuy Gift Card." Beneath that instruction, the page displayed a pre-filled FedEx shipping label containing the undercover name and address I used on the previous website. To the left of this label was the message "$1000 Best Buy Gift Card!" and an image of the BestBuy Gift Card. I clicked on the button labeled "Send It!" for the shipping of my $1000 Best Buy gift card. McKenney Att. B, at 9.

25. After I clicked on this button, the webpage on the website http://bestdigitalrewards.com expanded, and I was informed that before I could claim my $1,000 gift card, I had to complete any two third-party offers listed on that page. I also proceeded to the next two pages, where there were more offers to sign up for, and where I was informed that I

needed to sign up for additional offers to claim the gift card. Most of the offers listed on these pages stated that I needed to pay a fee to participate. McKenney Att. B, at 10-13 and 29-36.

26. I proceeded to click on the advertisements for some of the third-party offers. In each instance, I was taken to a publicly available webpage on a different website, where I could sign up for the third-party offers. Some of these third-party offers had terms and conditions that were available by hyperlink. McKenney Att. B, at 14-21.

27. At the webpage on the website http://bestdigitalrewards.com, described in paragraphs 24-25 above, I also clicked on a hyperlink labeled "Terms and Conditions." I was directed to the publicly available webpage http://bestdigitalrewards.com/terms.php. McKenney Att. B 22-28.

lbit.biz - bestgiftcardsforu.com - mywebrewardsclub.com

28. In May 2012, an undercover cell phone operated by the FTC's regional office in Cleveland, Ohio, received an unsolicited text message from phone number 716-207-7937. The text message stated "Your entry last month has WON! Goto http://www.bestbuy.com.lbit.biz/?claimid=212 and enter your Winning Code: "6655" to claim your FREE $1,000." On May 21, 2012, from the FTC's office in Chicago, I entered the publicly available website http://www.bestbuy.com.lbit.biz/?claimid=212 into a web browser based on the unsolicited text message. I used Adobe and Snagit to capture the website http://www.bestbuy.com.lbit.biz/?claimid=212 as well as other websites linked to from this publicly available website. True and correct printouts of the captured websites, dated May 21, 2012, are attached hereto as **McKenney Att. C**. Undercover information has been redacted from the attachment.

29. This website displayed a message at the top of the web page stating "Get a $1,000 Bestbuy Gift Card!" Beneath that message was a message stating "15 of 1000 left" and an image of a Best Buy gift card. Beneath that image was the instruction "Please enter your code below" and a blank in which to do so, with a button labeled "Continue" next to it. Based on the complaint I had seen, I entered the code "6655." This website then displayed, in place of the instruction to enter my code and the blank in which to do so, the message "Your code is being validated... please stand by!" This website then displayed the message, "You have a Winning Code! Now sending you to claim your giftcard!" McKenney Att. C, at 1-3.

30. I was then redirected to a page at the website http://bestbuy.bestgiftcardsforu.com/. According to my web browser, the title of that page was, "Claim Your FREE $1,000 BestBuy Gift Card!" That page said "Get a FREE $1000 Best Buy Gift Card." Surrounding this message were several images, including the Best Buy logo, a photograph of a supposed Best Buy employee, an image of a Best Buy gift card, and images of a Samsung flat-screen television, an Apple iPad, another Apple product such as an iPhone or iPod, and a Canon camera. Beneath the two messages, the website instructed, "Enter Your E-mail Address:" and included a space in which to do so. Beneath that button was a space marked "CONTINUE." At the bottom of this web page and several additional pages attached as McKenney Att. C was identical or nearly identical text to the text quoted in paragraph 11, above, as well as links to identical or nearly identical "Representative Sample," "Terms and Conditions," and "Privacy Policy" pages described in paragraphs 12 through 14 above. McKenney Att. C, at 4.

31. I inputted an undercover email address in the blank, then pressed "CONTINUE." I immediately was directed to another page on the same website,

http://bestbuy.bestgiftcardsforu.com/p2.php. According to my web browser, the title of that page also was, "Claim Your FREE $1,000 BestBuy Gift Card!" That website stated, "Congratulations! Tell us where to send your $1000 BestBuy Gift Card!" Beneath that message, the website requested additional personal information from me, including my gender, name, address, email address, date of birth, cell phone numbers. I filled in the required fields using undercover information and clicked a button marked "Continue." McKenney Att. C, at 5-6.

32. I then was redirected to a webpage on the website http://mywebrewardsclub.com/. This page told me that I was at the "Last Step," and instructed me to "Tell us where to ship your $1000 BestBuy Gift Card." Beneath that instruction, the page displayed a pre-filled FedEx shipping label containing the undercover name and address I used on the previous website. To the left of this label was the message "Receive a $1000 Best Buy Gift Card" and an image of the Best Buy gift card. After I clicked on the button labeled "Send It!" for the shipping of my $1000 Best Buy gift card, the web page expanded, and I was informed that before I could claim my $1000 gift card, I had to complete two of several third-party offers listed on that page. I also proceeded to the next two pages, where there were more offers to sign up for, and where I was informed that I needed to sign up for a total of 11 additional offers to claim the gift card. Several of the offers listed on these pages stated that I needed to pay a fee to participate. Several of the offers had terms and conditions, accessible only by hyperlink, providing for a so-called "negative option" whereby ordering a trial of the product would enroll me to continue to receive and be charged for the product until I canceled. McKenney Att. C, at 7-17.

bit.lyUyubPt - yourfreegiftshop.com

33. On February 8, 2013, I received on my FTC-issued cell phone, an unsolicited text message from the shortcode 4162 stating "clarosirovs@aol.com / Tyler / Your phone last day is 1ST! Go to http://bit.ly/UyubPt and put 6371 to request your prize."

34. On February 11, 2013, from the FTC's office in Chicago, I entered the link listed in the unsolicited text message http://bit.ly/UyubPt into a web browser. Upon entering that link, I was redirected to the publicly available website http://bestbuy.yourfreegiftshop.com/p1?reqid=28130384&affid=55&oid=13&s1=269582&s2=&email=. According to the web browser I was using, this page was entitled "Free $1,000 Best Buy Gift Card." I used Adobe and Snagit to capture this website as well as other websites linked to from this website. True and correct printouts of these captured websites, dated February 11, 2013, are attached hereto as **McKenney Att. D**. Undercover information has been redacted from the attachment.

35. At the top of this web page was a message stating, "Get a Free BEST BUY Gift Card." Under the message was another message stating, "Congratulations! You Qualify for a FREE $1,000 Best Buy Gift Card." Next to these two messages were several images, including an image of a Best Buy gift card with "$1,000" printed on it and images of a flat-screen television, an Apple laptop computer, another Apple product such as an iPhone or iPod, and a Canon camera. Beneath the two messages, the website instructed, "Enter Your E-mail Address:" and included a space in which to do so. Beneath that space was a button marked "CONTINUE." At the bottom of this web page and several additional pages attached as McKenney Att. D was identical or nearly identical text to the text quoted in paragraph 11, above, as well as links to

identical or nearly identical "Representative Sample," "Terms and Conditions," and "Privacy Policy" pages described in paragraphs 12 through 14 above. McKenney Att. D, at 1.

36. Where prompted to enter my email address, as described in paragraph 35 above, I entered an undercover email address that I had created that day, clicked on the button marked "CONTINUE," and was directed to another page on the same website, http://bestbuy.yourfreegiftshop.com/common/rpb?stc=2&oid=13&email=[email address], with the undercover email address in place of the [email address] in the website address above. This page repeated the message "Get a Free BEST BUY Gift Card" and beneath that included the same image of a Best Buy gift card with "$1,000" printed on it. This page also had a message about receiving a "Best Buy Newsletter." This page also stated, "STEP 2: You're on your way to claiming your $1,000 Best Buy Gift Card. To ensure delivery, please enter your correct shipping information below:". In bold letters, the page then stated, "Tell us where to send your $1,000 Best Buy Gift Card." The page requested additional personal information from me, including my name, address, date of birth, and cell phone number. The page also asked me certain questions, such as "Are you interested in going back to school?" and "Are you diabetic?," with buttons labeled "yes" and "no" next to each question. In each instance, I chose "no." Beneath the blanks for this information was a button marked "CONTINUE." McKenney Att. D, at 2-3.

37. I filled in the required fields using undercover information and clicked "CONTINUE." I was then sent through several additional pages on the website http://bestbuy.yourfreegiftshop.com, which included offers for a credit card, a cell phone, and several dozen additional products and services. In each instance, I was asked to indicate whether I wanted more information on the offer; in each instance, I selected "no." Each additional page

was labeled according to the "Step" I had reached, such as "Step 3," "Step 4," or "Final Step." McKenney Att. D, at 4-12.

38. Finally, I reached a page on the website http://bestbuy.yourfreegiftshop.com labeled "Final Steps." This page displayed a pre-filled FedEx shipping label containing the undercover name and address I used on the previous website. Beneath that information was a button labeled "Send It!" McKenney Att. D, at 13.

39. I clicked the button labeled "Send It!" for the shipping of my $1,000 Best Buy Gift Card, and the web page immediately expanded. Once again, the undercover information I had entered was displayed, but now the message said "$1,000 Best Buy Gift Card Reserved For:". Beneath the contact information I entered, I was told "Finish by completing any 2 offers below to claim your $1,000 Best Buy Gift Card." Beneath that message were links to several third-party offers. Each offer had an image and a message such as "Only $1.00" or "Just Pay Shipping." McKenney Att. D, at 13-17.

40. I scrolled to the bottom of the webpage and saw the message "You are on the Silver offer page," as well as buttons labeled "Go to Gold Offers" and "Go to Platinum Offers." I clicked on the "Go to Gold Offers" button and was taken to http://bestbuy.yourfreegiftshop.com/common/rpw?is_submit=2, which was very similar to the "Silver Offer" page, including the label "FINAL STEPS," the image of a $1000 Best Buy gift card, the message that the gift card was reserved for the undercover name I had submitted, and below, the message "Finish by completing any 2 offers below to claim your $1,000 Best Buy Gift Card." McKenney Att. D, at 18-22.

41. I scrolled to the bottom of the webpage described in paragraph 40 and saw the message, "You are on the Gold offer page," as well as buttons labeled "Go to Silver Offers" and

"Go to Platinum Offers." I clicked on the "Go to Platinum Offers" button and http://bestbuy.yourfreegiftshop.com/common/rpw?is_submit=3, which was very similar to the "Silver Offer" and "Gold Offer" pages, including the label "FINAL STEPS," the image of an $1000 Best Buy gift card, the message that the gift card was reserved for the undercover name I had submitted, and below, the message "Finish by completing any 2 offers below to claim your $1,000 Best Buy Gift Card." McKenney Att. D, at 23-27.

UNSOLICITED EMAIL

42. On February 11, 2013, I created an undercover email address. Also on February 11, 2013, as discussed in paragraph 36 above, I visited the publicly available website bestbuy.yourfreegiftshop.com/p1. At that website, once prompted to put in my email address, I inputted the undercover email address I had created earlier that day. I did not use or disclose the undercover email address in any other way. Between February 11, 2013 and February 18, 2013, that undercover email address received at least 411 emails. All or nearly all of these emails were unsolicited commercial emails, and all were delivered to the undercover email address after I submitted the email address on the publicly available website bestbuy.yourfreegiftshop.com/p1, as described in paragraph 16, above.

43. These emails promoted a wide variety of products and services. Some examples of those emails subject lines are: "Lose weight with this 1 simple ingredient!"; "You've received $100 - $1000 Cash"; "Melt Fat Away – Trick Your Brain Into BEING THIN!"; "Need Cash Quick? Get up to $1000 Now – Open 365 Days A Year!"; "My Russian Bride webcam is now live for [undercover email address]!"; and "Increase your sexual stamina with Vydox."

BUSINESS RECORDS AND LISTINGS

SubscriberBASE Holdings

44. On January 9, 2013, I obtained business records for SubscriberBASE Holdings through the South Carolina Secretary of State. Attached hereto as **McKenney Att. E** is a true and correct copy of certain business records for SubscriberBASE Holdings including Articles of Incorporation; Articles of Amendment dated June 21, 2002; a Notice of Change of Registered Office or Registered Agent or Both of a South Carolina or Foreign Corporation dated February 14, 2005; and a Notice of Change of Registered Office or Registered Agent or Both of a South Carolina or Foreign Corporation dated April 19, 2011. According to these records:

a. On May 19, 2000, a corporation called PriceJester, Inc. was formed with Jeffrey L. French as its registered agent and one of its two incorporators (McKenney Att. E, at 1-2);

b. On May 17, 2002, PriceJester, Inc. changed its name to SubscriberBASE Holdings (McKenney Att. E, at 3-4);

c. On February 14, 2005, SubscriberBASE Holdings, with Jeffrey L. French as its President, changed its registered address to 3830 Forest Drive, Suite 207, Columbia, South Carolina 29204 (McKenney Att. E, at 5-6); and

d. On April 19, 2011, SubscriberBASE Holdings changed its registered agent to CT Corporation System and its registered address to 2 Office Park Court, Suite 103, Columbia, South Carolina 29223 (McKenney Att. E, at 7-8).

SubscriberBASE

45. On January 9, 2013, I obtained business records for SubscriberBASE through the South Carolina Secretary of State. Attached hereto as **McKenney Att. F** is a true and correct copy of certain business records for SubscriberBASE including Articles of Incorporation; a Notice of Change of Registered Office or Registered Agent or Both of a South Carolina or Foreign Corporation dated February 14, 2005; and a Notice of Change of Registered Office or Registered Agent or Both of a South Carolina or Foreign Corporation dated April 19, 2011. According to these records:

a. On July 24, 2000, SubscriberBASE was formed with Jeffrey L. French as its registered agent and one of its two incorporators (McKenney Att. F, at 1-2);

b. On February 14, 2005, SubscriberBASE, with Jeffrey L. French as its President, changed its registered address to 3830 Forest Drive, Suite 207, Columbia, South Carolina 29204 (McKenney Att. F, at 3-4); and

c. On April 19, 2011, SubscriberBASE changed its registered agent to CT Corporation System and its registered address to 2 Office Park Court, Suite 103, Columbia, South Carolina 29223 (McKenney Att. F, at 5-6).

CMB Marketing, Inc.

46. On December 17, 2012, I obtained a publicly available business record listing for CMB Marketing, Inc. ("CMB Marketing") through the New York Department of State's website, http://www.dos.ny.gov/corps/bus_entity_search.html. Attached hereto as **McKenney Att. G** is a true and correct copy of that publicly available business record listing. According to this listing:

a. the Chairman or Chief Executive Officer of CMB Marketing is Christopher McVeigh (McKenney Att. G, at 1); and

b. the Principal Executive Office of CMB Marketing is: Christopher McVeigh, 67 Old Oak Rd, Warwick, New York 10990 (McKenney Att. G, at 1).

All Square Marketing

47. On May 23, 2012, I obtained a publicly available business record listing for All Square Marketing through the California Secretary of State's website, http://kepler.sos.ca.gov/. Attached hereto as **McKenney Att. H** is a true and correct copy of that publicly available business record listing. According to this listing, All Square Marketing's registered address is 24000 Alicia Parkway, Suite 17-433, Mission Viejo, CA 92961.

Threadpoint

48. On October 19, 2012, I obtained a publicly available business record listing for Threadpoint through the California Secretary of State's website, http://kepler.sos.ca.gov/. Attached hereto as **McKenney Att. I** is a true and correct copy of that publicly available business record listing. According to this listing, Threadpoint's registered address is 24881 Alicia Parkway, Suite E 310, Laguna Hills, CA 92653.

PC Global

49. On October 16, 2012, I obtained a publicly available business record listing for PC Global through the California Secretary of State's website, http://kepler.sos.ca.gov/. Attached hereto as **McKenney Att. J** is a true and correct copy of that publicly available business record listing. According to this listing, PC Global's registered address is 27068 La Paz Rd Ste 566, Aliso Viejo, CA 92656.

BANK RECORDS

SubscriberBASE Holdings

50. On November 21, 2012 and January 4, 2013, pursuant to a CID, Branch Banking and Trust Company ("BB&T") produced certain records concerning 22 accounts held in the name of or otherwise related to SubscriberBASE Holdings. The records produced by BB&T included records related to a business account held in the name of SubscriberBASE Holdings with an account number ending -8328. The records related to the -8328 SubscriberBASE Holdings account included signature cards, monthly account statements through October 31, 2012, and records of certain wire transfers, images of checks, and deposit and withdrawal slips through November 30, 2012.

51. BB&T Signature Cards for at least 11 of the 22 accounts are signed by Jeffrey French as President of SubscriberBASE Holdings.

52. The bank records for the SubscriberBASE Holdings -8328 account show transfers related to All Square Marketing and Threadpoint, including at least the following transfers:

Date	Transferor	Transferee	Amount
Oct. 7, 2011	SubscriberBASE Holdings	All Square Marketing	$ 22,131.26
Nov. 18, 2011	SubscriberBASE Holdings	All Square Marketing	$ 105,210.35
Dec. 8, 2011	SubscriberBASE Holdings	All Square Marketing	$ 124,478.50
Jan. 4, 2012	SubscriberBASE Holdings	All Square Marketing	$ 133,197.34
Feb. 6, 2012	SubscriberBASE Holdings	All Square Marketing	$ 258,716.26
Mar. 6, 2012	SubsceribBASE Holdings	All Square Marketing	$ 119,775.38
Apr. 3, 2012	SubscriberBASE Holdings	All Square Marketing	$ 27,933.59
Apr. 4, 2012	SubscriberBASE Holdings	All Square Marketing	$ 76,234.83
Apr. 9, 2012	SubscriberBASE Holdings	Threadpoint	$ 7,494.95
May 7, 2012	SubscriberBASE Holdings	All Square Marketing	$ 134,548.13
Jun. 1, 2012	SubscriberBASE Holdings	All Square Marketing	$ 300,000.00
Jun. 4, 2012	SubscriberBASE Holdings	All Square Marketing	$ 149,917.68
Jul. 3, 2012	SubscriberBASE Holdings	All Square Marketing	$ 187,048.30
Jul. 30, 2012	SubscriberBASE Holdings	Threadpoint	$ 5,802.49
Aug. 3, 2012	SubscriberBASE Holdings	Threadpoint	$ 215,905.51
Sept. 6, 2012	SubscriberBASE Holdings	Threadpoint	$ 62,647.88
Oct. 5, 2012	SubscriberBASE Holdings	All Square Marketing	$ 68,566.13

Nov. 7, 2013	SubscriberBASE Holdings	All Square Marketing	$ 206,333.13
		Total:	**$ 2,205,941.71**

53. The bank records for the SubscriberBASE Holdings -8328 also show the transfers related to two business accounts maintained by Cole Taylor Bank in Chicago, Illinois in the name of Eagle Web Assets in Rosemont, Illinois, including at least 65 transfers totaling $569,834.50.

All Square Marketing, Threadpoint, PC Global, and Slash 20

54. On November 30, 2012, pursuant to a CID, JPMorgan Chase Bank, N.A. ("Chase") produced certain records concerning:

a. a business account held in the name of All Square Marketing with an account number ending -6856;

b. three business accounts held in the name of Threadpoint with account numbers ending -6997, -8717, and -9681; and

c. a business account held in the name of PC Global with an account number ending -6948.

These records included signature cards, monthly account statements, and images of checks, deposit and withdrawal slips through October 31, 2012.

55. On November 7, 2012, pursuant to a CID, Chase produced certain records concerning a business account held in the name of Slash 20 with an account number ending -6872. The records included signature cards, monthly account statements, and images of checks, deposit and withdrawal slips through September 30, 2012.

All Square Marketing

56. The Business Signature Card for All Square Marketing's Chase account:

a. lists only one signatory, Christopher S Pothier; and

b. indicates that the account was opened on August 9, 2011 at Chase's Aliso Viejo location.

57. The bank records for All Square Marketing's Chase account show the transfers from SubscriberBASE Holdings to All Square Marketing described in paragraph 52 above, except the November 7, 2013 transfer, which came after the last date of Chase's production. This account also shows the following transfers, among others:

a. at least 18 transfers totaling at least $540,000 from Threadpoint to All Square Marketing's Chase account;

b. at least 10 transfers totaling at least $900,000 from All Square Marketing's Chase account to Threadpoint's Chase accounts;

c. at least 23 transfers totaling at least $440,000 from All Square Marketing's Chase account to PC Global's Chase account;

d. at least 23 transfers totaling at least $351,000 from All Square Marketing's Chase account to CMB Marketing;

e. at least 22 transfers totaling at least $133,000 from All Square Marketing's Chase account to Mazzco Marketing, Inc.; and

f. at least 24 transfers totaling at least $125,000 from All Square Marketing's Chase account to a business account maintained by Cole Taylor Bank in Chicago, Illinois in the name of Eagle Web Assets in Rosemont, Illinois.

Threadpoint

58. The Business Signature Card for Threadpoint's -6997 account:

a. lists only one signatory, Christopher S Pothier; and

b. indicates that the account was opened on August 9, 2011 at Chase's Aliso Viejo location.

59. The Business Signature Card for Threadpoint's -8717 account:

a. lists only one signatory, Christopher S Pothier; and

b. indicates that the account was opened at Chase's Aliso Viejo location.

60. The Business Signature Card for Threadpoint's -9681 account:

a. lists only one signatory, Christopher S Pothier; and

b. indicates that the account was opened at Chase's Aliso Viejo location.

61. The bank records for the three Threadpoint accounts show the following transfers, among others:

a. the transfers from SubscriberBASE Holdings to Threadpoint identified in paragraph 52 above;

b. the transfers between All Square Marketing and Threadpoint described in paragraph 57(a)-(b) above;

c. at least 31 transfers totaling at least $940,000 from Threadpoint's Chase accounts to PC Global's Chase account;

d. at least 10 transfers totaling at least $385,000 from Threadpoint's Chase accounts to Slash 20's Chase account;

e. at least 13 transfers totaling at least $127,000 from Threadpoint's Chase accounts to CMB Marketing;

f. at least 9 transfers totaling at least $44,000 from Threadpoint's Chase accounts to Mazzco Marketing, Inc.; and

g. at least 20 transfers totaling at least $67,000 from Threadpoint's Chase accounts to two business accounts maintained by Cole Taylor Bank in Chicago, Illinois in the name of Eagle Web Assets in Rosemont, Illinois.

PC Global

62. The Business Signature Card for PC Global's Chase account::

a. lists only one signatory, Christopher S Pothier; and

b. indicates that the account was opened on August 9, 2011 at Chase's Aliso Viejo location.

63. The bank records for PC Global's Chase account show, among other transfers:

a. the transfers from All Square Marketing's Chase account to PC Global's Chase account, described in paragraph 57(c) above;

b. the transfers from Threadpoint's Chase account to PC Global's Chase account, described in paragraph 61(c) above; and

c. at least 14 transfers totaling at least $262,000 from PC Global's Chase account to Slash 20's Chase account.

Slash 20

64. The Business Signature Card for Slash 20's Chase account:

a. lists only one signatory, Christopher S Pothier;

b. indicates that the account was opened on August 9, 2011; and

c. indicates that the account was opened at Chase's Aliso Viejo location.

PAYPAL RECORDS

65. On or about July 13, 2012, pursuant to a CID, PayPal, Inc. ("PayPal") produced certain records to the FTC concerning a PayPal account registered to Brent Cranmer and Slash 20. Those PayPal records show, among other things, the following:

a. The user of the account is identified as Brent Cranmer;

b. The Business Name associated with the account is Slash 20;

c. The first address listed with the account is Slash 20, LLC, 27068 La Paz Rd, Suite 566, Aliso Viejo, CA 92656;

d. An American Express credit card in the name of Brent Cranmer with an account number ending -4188 is linked to the PayPal account; and

e. The account had been logged into 1288 times through the Internet Protocol ("IP") address 98.191.147.2. The first time that the account had been logged into from that IP address was March 4, 2011, when the account was established. At the time of PayPal's production, the account most recently had been logged into from that IP address on July 13, 2012, the same day as the production. The account also had been logged into a total of 88 times from 32 different IP addresses.

INTERNET SERVICE PROVIDER (ISP) RECORDS

66. On or about November 30, 2012, pursuant to a CID, CSC Holdings LLC ("CSC") produced certain records to the FTC concerning two Internet service accounts. CSC maintains these and other Internet service accounts through its subsidiary, Optimum Online. A true and correct copy of these records is attached hereto as **McKenney Att. K**. Sensitive personal information has been redacted from McKenney Att. K. The records produced by CSC show:

a. That the IP address 96.56.219.2 was assigned to CMB Marketing (McKenney Att. K, at 1); and

b. That the IP address 24.184.238.167 was assigned to Michael Mazzella between May 14, 2012 and June 9, 2012 (McKenney Att. K, at 2-7).

INTEGRACLICK, LLC

67. On or about October 11, 2012, pursuant to CID, IntegraClick, LLC, which also does business as Clickbooth ("Clickbooth"), produced certain records to the FTC concerning online advertising campaigns that were operated through its affiliate network. A true and correct copy of some of these records is attached as **McKenney Att. L**. Sensitive personal information has been redacted from McKenney Att. L. The records produced by Clickbooth show:

a. All Square Marketing advertised gift card promotions through Clickbooth (McKenney Att. L, at 1-8);

b. Clickbooth sent these invoices to the attention of Mike Mazzella (McKenney Att. L, at 1-8);

c. On these invoices, Clickbooth also lists an email address for All Square Marketing of mike@allsquaremarketing.com (McKenney Att. L, at 1-8);

d. Clickbooth used the address 24000 Alicia Pkwy., Suite #17-433, Mission Viejo, CA 92691 for All Square Marketing (McKenney Att. L, at 1-8);

e. On August 26, 2011, All Square Marketing paid Clickbooth $15,000 by an American Express credit card in the name of Brent Cranmer with an account number ending -188 (McKenney Att. L, at 9-11);

f. On August 26, 2011, Mike Mazzella, from the email address mmazzella@allsquaremarketing.com, forwarded to a Clickbooth representative an

email exchange between Mazzella, Brent Cranmer, Chris McVeigh, and two additional individuals, Lauren Hoon and Rob Nicolosi (McKenney Att. L, at 12-13);

g. In that email exchange, Brent Cranmer has an email signature indicating that he is "Senior Finance Manager" at "PC Investments" (McKenney Att. L, at 12);

h. Cranmer submitted his driver's license with the $15,000 payment (McKenney Att. L, at 14);

i. A document entitled "Clickbooth Advertiser Compliance Questionnaire" was signed by Michael Mazzella as Vice President of All Square Marketing (McKenney Att. L, at 15-16);

j. A document entitled "Clickbooth.com Advertiser Terms and Conditions" was signed by Michael Mazzella as Vice President of All Square Marketing, and also lists an email address of mike@allsquaremarketing.com (McKenney Att. L, at 17-19);

k. Two documents entitled "Advertising Insertion Order," dated August 15, 2011 and January 18, 2012, were signed by Michael Mazzella as Vice President of All Square Marketing (McKenney Att. L, at 20-21); and

l. A document entitled "DNBI Risk Management," and dated August 2, 2011, lists Chris McVeigh under the "Contact Information" for All Square Marketing (McKenney Att. L, at 22-23).

LINKEDIN PROFILE

68. On or about November 1, 2012, I went to the publicly available website http://www.linkedin.com/pub/brent-cranmer/8/733/102?trk=pub-pbmap, where I found a LinkedIn profile for Brent Cranmer. A true and correct copy of that profile is attached here as **McKenney Att. M**. In this profile, Cranmer identifies himself as the "Controller/Senior Finance Manager" at PC Global.

NAMECHEAP, INC.

69. On June 18, July 24, and November 29, 2012, pursuant to CID, NameCheap, Inc. ("NameCheap") produced certain records to the FTC concerning website domain names that were registered through NameCheap. Excerpts of those records have been produced to the court separately, attached to the Certificate of Authenticity of Business Records of Sergio Hernandez.

70. The records produced by NameCheap include registration records for several websites that FTC staff captured during the course of the investigation, including myrewards2day.com (discussed in paragraphs 10-16 above), myrewardshouse.com (discussed in paragraphs 22-23 above) and bestgiftcardsforu.com (discussed in paragraphs 30-31 above). These registration records included the account used to register the website, the person paying for the registration of the website and the method of payment, and the IP address from which the website was registered and from which the NameCheap account in question was later accessed. The registration records produced by NameCheap show the following screen name and payment information for some of the websites captured by FTC staff during the course of the investigation:

Domain Name	NameCheap Account	Paid for by	Payment method
bestgiftcardsforu.com	mazzco	Mike Mazzella	Credit Card
mygiftcardsnow.com	mazzco	Mike Mazzella	Credit Card
oursuperoffersnow.com	newwavemedia2121	Slash 20, LLC/Brent Cranmer	PayPal
thebestsiteforgiftcards.com	newwavemedia2121	Slash 20, LLC/Brent Cranmer	PayPal
thetopoffers4u.com	newwavemedia212	Slash 20, LLC/Brent Cranmer	PayPal
thetopoffersforu.com	newwavemedia212	Slash 20, LLC/Brent Cranmer	PayPal
thegiftcarddeal.com	squaremarketing	Slash 20, LLC/Brent Cranmer	PayPal
myrewardshouse.com	carrysings	Slash 20, LLC/Brent Cranmer	PayPal
newrewardsdaily.com	carrysings	Slash 20, LLC/Brent Cranmer	PayPal
myrewards2day.com	joanntracey	Slash 20, LLC/Brent Cranmer	PayPal

71. Each of these websites, when visited by FTC staff and as captured FTC staff, promoted "free" gift cards or other merchandise in a manner similar to the websites myrewards2day.com, myrewardshouse.com/ and bestgiftcardsforu.com/. Acting on consumer complaints of unsolicited text messages, FTC staff made over forty captures of the websites listed in the table in paragraph 70 over a period that lasted more than six months.

72. In making at least 17 captures of websites registered through the NameCheap accounts above, FTC staff was redirected to those websites through the website squareclk.com. When FTC staff was redirected through the website squareclk.com, it displayed no content, and instead appeared to be used for tracking. Once FTC staff was redirected to the website squareclk.com, staff was immediately and automatically redirected to the website that promoted "free" gift cards or other merchandise. According to the NameCheap records, squareclk.com was registered through the "squaremarketing" account and paid for using the Slash 20/Brent Cranmer PayPal account.

73. The NameCheap records also showed the following:

a. The websites bestgiftcardsforu.com and mygiftcardsnow.com, both registered by Mike Mazzella, were registered from the IP address 96.56.219.2, discussed in this declaration at paragraph 66(a) above;

b. The "mazzco" and "newwavemedia2121" NameCheap accounts both have been accessed from the IP address, 24.184.238.167, discussed in this declaration at paragraph 66(b) above;

c. The websites myrewardshouse.com, newrewardsdaily.com, and myrewards2day.com, all of which were paid for through the Slash 20, LLC/Brent Cranmer PayPal account, all were registered from the IP address 98.191.147.2;

d. the NameCheap account "carrysings" also was used to purchase the website dailygiftcard.com; and

e. The NameCheap accounts "mazzco," "newwavemedia2121," "squaremarketing," "carrysings" and "joanntracey" all have been accessed from the IP address 98.191.147.2 multiple times since May 1, 2012.

WEBSITE HOSTING RECORDS

74. On February 15, 2013, I visited the publicly available website DomainTools at www.DomainTools.com. DomainTools provides information through its "whois" search engine about the ownership of domain names, including, among other things, the name and address of the domain name registrant, the administrative and technical contacts, the registrar that registered the domain on behalf of the registrant, the date the domain name was registered, the IP address of the web server hosting the domain name, and a "Reverse IP" function that shows all websites hosted at a particular IP address. On that website, I searched for the hosting history of

freegiftcardworld.com and yourfreegiftshop.com. A true and correct copy of records from DomainTools are attached here as **McKenney Att. N**. According to DomainTools:

a. on February 11, 2013, the date I captured the website yourfreegiftshop.com as described in paragraphs 34 through 41 above, that website, was registered through NameCheap (McKenney Att. N, at 1-2);

b. from February 7, 2013 until at least February 15, 2013, yourfreegiftshop.com was hosted at the IP address 5.39.219.61 (McKenney Att. N, at 3); and

c. at that time the IP address 5.39.219.61 hosted only two websites, yourfreegiftshop.com and freegiftcardworld.com (McKenney Att. N, at 4).

75. On January 4, 2013, FTC staff visited DomainTools. As of that date, according to DomainTools, the IP address 5.39.219.0 hosted only three websites: freegiftcardworld.com, myrewards2day.com, and newrewardsdaily.com (McKenney Att. N, at 5). Both myrewards2day.com and newrewardsdaily.com, as noted in the table in paragraph 70, above, were registered through NameCheap and paid for using the Brent Cranmer/Slash 20 PayPal account.

SUBSCRIBERBASE PRESS RELEASE

76. On or about January 2, 2013, I visited the publicly available website http://www.subscriberbase.com/offlineexpansion052708.html. There, I found a document dated May 27, 2008 and entitled "SubscriberBASE Announces Expansion of Offline Marketing Division in Chicago." A true and correct copy of that document is attached hereto as **McKenney Att. O**.

CONSUMER COMPLAINTS

77. The FTC maintains Consumer Sentinel, a database of consumer complaints that can be accessed by the FTC and other law enforcement agencies. The consumer complaints in Consumer Sentinel come from federal, state, local and international law enforcement agencies and private organizations. Individual consumers can file complaints with the FTC by phone, mail or through its website http://www.ftc.gov.

78. During the course of the investigation, FTC staff accessed Consumer Sentinel and identified numerous complaints from consumers who filed complaints concerning:

a. the domain names identified in paragraphs 73 through 76 above;

b. mywebrewardsclub.com and bestdigitalrewards.com; and

c. the names "SubscriberBASE Holdings;" SubscriberBASE;" "All Square Marketing," "Threadpoint," "PC Global;" and "Slash 20."

A true and correct copy of some of those complaints is attached hereto as **McKenney Att. P**. Personal identifying information has been redacted from this attachment.

79. During the course of the investigation, I accessed Consumer Sentinel and conducted searches on the number of complaints received annually about unsolicited text messages claiming consumers won a free prize. The results are, in 2012, Consumer Sentinel received at least 20,000 consumer complaints involving the receipt of unsolicited text messages claiming consumers won a free prize such as a gift card or merchandise. This represents a significant increase from the year before, when in 2011, Consumer Sentinel received only 2700 consumer complaints involving the receipt of unsolicited text messages claiming consumers won a free prize such as a gift card or merchandise.

ADDITIONAL TEXT MESSAGE SPAM

80. In addition to text messages described elsewhere in this declaration, this investigation has uncovered additional unsolicited text messages that were received in this judicial district. Some of these messages are attached hereto as **McKenney Att. Q**.

81. On June 4, 2012, an unsolicited text message was received by a family member of FTC staff on a personal cell phone stating, "Dear Walmart shopper, your purchase last month won a $1OOO [sic] Walmart Gift Card, go to www.vCardSpot.com within 24 hours to claim. (NO2Cancel)". (McKenney Att. Q, at 1.) Also on June 4, 2012, from the FTC's office in Chicago, I entered www.vCardSpot.com, the link listed in the unsolicited text message, into a web browser. After submitting undercover personal information, I was taken to the publicly available website thegiftcarddeal.com and, in turn, to the publicly available website mywebrewardsclub.com. As noted in the table in paragraph 70 above, thegiftcarddeal.com was registered with NameCheap through the "squaremarketing" account and paid for using the Brent Cranmer/Slash 20 PayPal account.

82. On May 27, 2012, I received on my FTC-issued cell phone, an unsolicited text message from (360) 362-3424 stating, "Your entry last month has WON! Go to http://bit.ly/Jyu6kE and enter your Winning Code: '1122' to claim your FREE $1,000 Best Buy Giftcard [sic]!" (McKenney Att. Q, p. 2.) Also on May 29, 2012, from the FTC's office in Chicago, I entered http://bit.ly/Jyu6kE, the link listed in the unsolicited text message, into a web browser. After submitting the "code" in the text message, I was taken to the publicly available website mygiftgardsnow.com. As noted in the table in paragraph 70 above, mygiftgardsnow.com was registered with NameCheap through the "mazzco" account and paid for using the with a credit card held in the name of Michael Mazzella.

STATE ATTORNEYS GENERAL

83. On September 10, 2012, FTC staff visited the website of the Washington State Office of the Attorney General, http://www.atg.wa.gov. At the URL http://www.atg.wa.gov/uploadedFiles/Home/News/Press_Releases/2008/SubscriberBASEConsentDecree043008.pdf, FTC staff found a Consent Decree from the case of *State of Washington v. SubscriberBASE Holdings, Inc., et al.*, 08-2-14566-2SEA. A true and correct copy of that Consent Decree is attached hereto as **McKenney Att. R**.

84. On September 10, 2012, FTC staff visited the website of the Florida Office of the Attorney General, http://www.myfloridalegal.com. At the URL http://myfloridalegal.com/webfiles.nsf/WF/JDAS-8M4RLK/$file/SubscriberBaseHoldingsAVCpdf.pdf, FTC staff found an Assurance of Voluntary Compliance in a matter in which the respondent is identified as SubscriberBASE Holdings, Inc. A true and correct copy of that Assurance of Voluntary Compliance is attached hereto as **McKenney Att. S**.

ARTICLES

85. On February 5, 2013, I accessed various websites containing articles about unsolicited text messages advertising supposedly free gift cards. Attached hereto as **McKenney Att. T** are true and correct printouts of these articles. These articles consist of:

a. An article entitled "Phony $1,000 Target Gift Card is the Scam of the Year," posted January 18, 2013, on AOL's Daily Finance website at: www.dailyfinance.com/2013/01/18/target-gift-card-is-the-scam-of-the-year/. (McKenney Att. T, pp. 1-5);

b. An article entitled "Text Message Gift Card Scam is Back for the Holidays," posted November 30, 2012, on the Better Business Bureau's website at: bbb.org/blog/2012/11/text-message-gift-card-scam-is-back-for-the-holidays/. (McKenney Att. T, pp. 6-8); and

c. An article entitled "How to stop scam messages from getting to your cell phone," posted January 28, 2013, on ABC15's website at: abc15.com/dpp/money/consumer/alerts/how-to-stop-scam-text-messages-from-getting-to-your-cell-phone. (McKenney Att. T, pp. 9-12).

I declare under penalty of perjury that the foregoing is true and correct.

Executed on February 28th, 2013

Douglas M. McKenney